CSE 312

Foundations of Computing II

Lecture 4: Counting pigeons, counting practice

Last Class: Counting

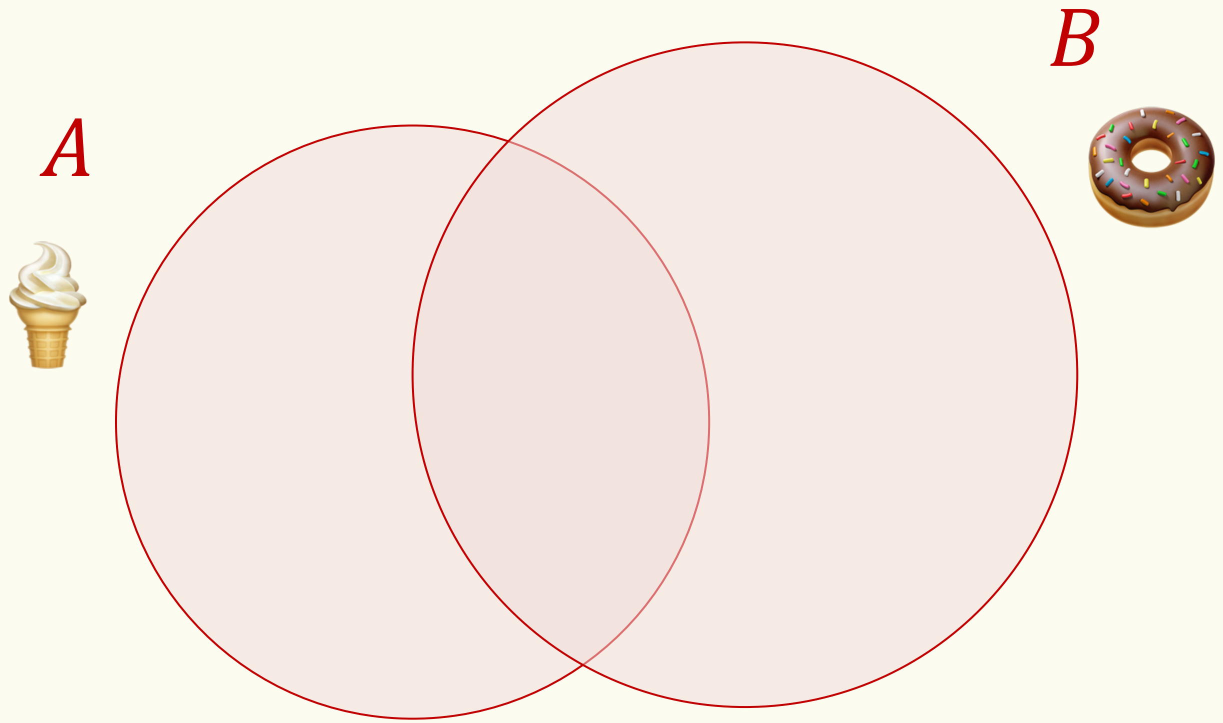
- Binomial Coefficients
- Binomial Theorem
- Inclusion-Exclusion

Today:

- Pigeonhole Principle
- Counting practice

Inclusion-Exclusion

But what if the sets are not disjoint?



$|A| = 43$
$|B| = 20$
$|A \cap B| = 7$
$|A \cup B| = ???$

Fact. $|A \cup B| = |A| + |B| - |A \cap B|$

Inclusion-Exclusion Example: RSA

Last time: For (distinct) primes p, q, and $N = p \cdot q$, how many integers in $\{0, \ldots, N-1\}$ have no common factor with N?

Idea:

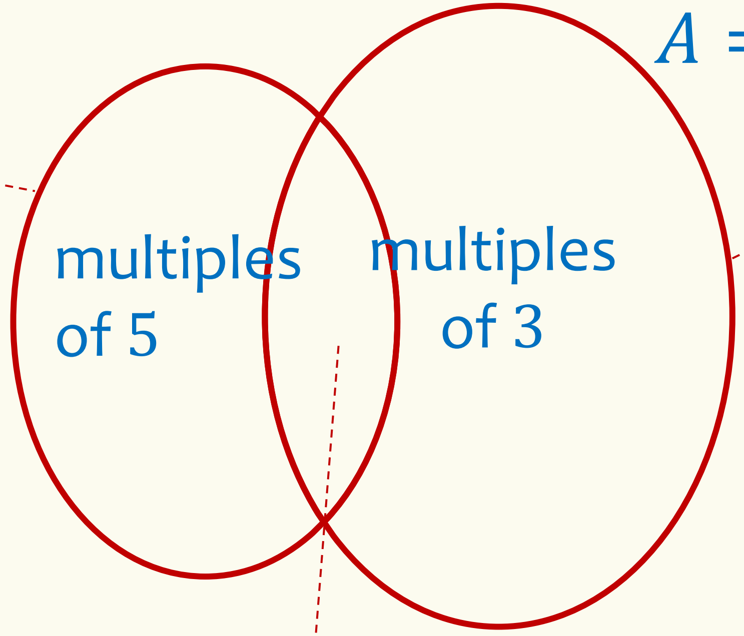
- $A =$ integers $\{0, \ldots, N-1\}$ divisible by p = multiples of p mod N
- $B =$ integers $\{0, \ldots, N-1\}$ divisible by q = multiples of q mod N
- Wanted: $N - |A \cup B|$

Example: $p = 3, q = 5 \quad N = 3 \times 5$

$B = \{0, 5, 10\}$

$A = \{0, 3, 6, 9, 12\}$

$|B| = 3$



$|A| = 5$

$A \cap B$ contains multiples of 3 & 5 (mod 15) $\quad A \cap B = \{0\}$

Integers between 0 and 14 that share a non-trivial divisor with 15
= $|A| + |B| - |A \cap B| = 3 + 5 - 1 = 7$

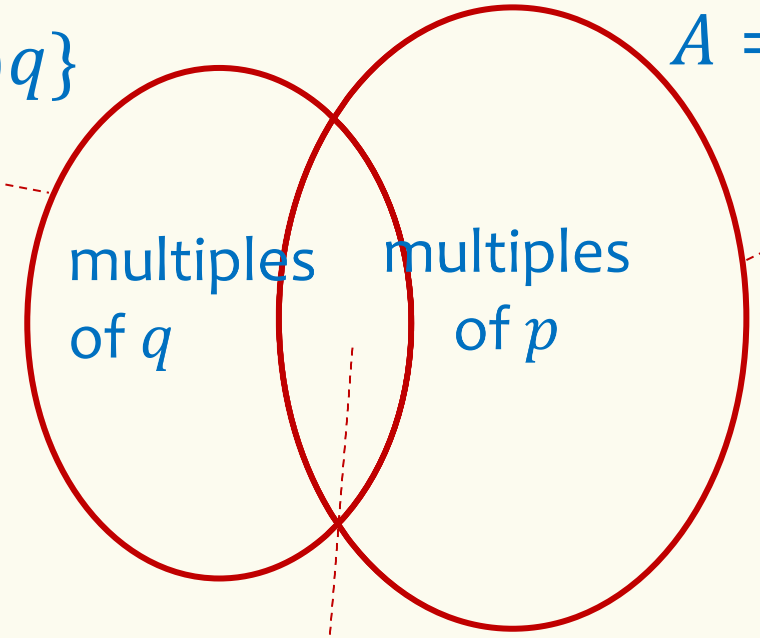
Integers between 0 and 14 that share no non-trivial divisor with 15
= $15 - 7 = 8$

More general: Integers mod N co-prime with $N = pq$ for p, q prime

$B = \{0, q, 2q, \ldots, (p-1)q\}$

$A = \{0, p, 2p, \ldots, (q-1)p\}$

$|B| = p$



$|A| = q$

$A \cap B$ contains multiples of p & q (mod N)

$A \cap B = \{0\}$

Integers between 0 and $N-1$ that share a non-trivial divisor with N
= $|A| + |B| - |A \cap B| = p + q - 1$

Integers between 0 and $N-1$ that are co-prime with N
= $N - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1)$

Last Class: Counting

- Binomial Coefficients
- Binomial Theorem
- Inclusion-Exclusion

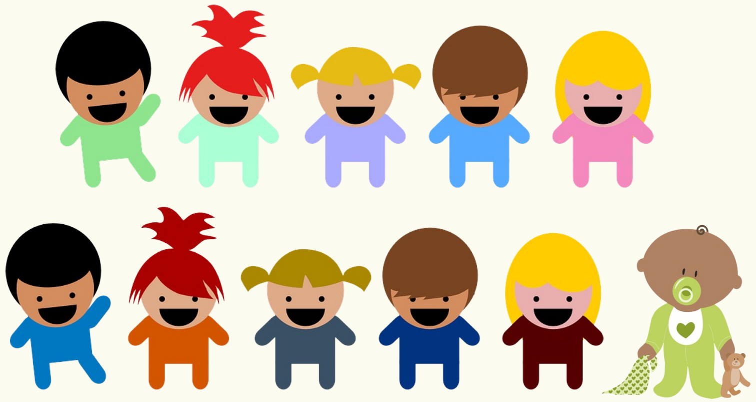
Today:

- Pigeonhole Principle
- Counting practice

Pigeonhole Principle (PHP): Idea

10 pigeons, 9 pigeonholes

Pigeonhole Principle: Idea



If 11 children have to share 3 cakes, at least one cake must be shared by how many children?

Pigeonhole Principle – More generally

If there are n pigeons in $k < n$ holes, then one hole must contain at least $\frac{n}{k}$ pigeons!

Proof. Assume there are $< \frac{n}{k}$ pigeons per hole.

Then, there are $< k \cdot \frac{n}{k} = n$ pigeons overall.

Contradiction!

Pigeonhole Principle – Better version

If there are n pigeons in $k < n$ holes, then one hole must contain at least $\left\lceil \frac{n}{k} \right\rceil$ pigeons!

Reason. Can't have fractional number of pigeons

Syntax reminder:

- Ceiling: $\lceil x \rceil$ is x rounded up to the nearest integer (e.g., $\lceil 2.731 \rceil = 3$)
- Floor: $\lfloor x \rfloor$ is x rounded down to the nearest integer (e.g., $\lfloor 2.731 \rfloor = 2$)

Pigeonhole Principle: Strategy

To use the PHP to solve a problem, there are generally 4 steps

1. Identify pigeons
2. Identify pigeonholes
3. Specify how pigeons are assigned to pigeonholes
4. Apply PHP

Pigeonhole Principle – Example

In a room with 367 people, there are at least two with the same birthday.

Solution:

1. **367** pigeons = people
2. **366** holes (365 for a normal year + Feb 29) = possible birthdays
3. Person goes into hole corresponding to own birthday
4. By PHP, there must be two people with the same birthday

Pigeonhole Principle – Example (Surprising?)

*In every set S of 100 integers, there are at least **two** elements whose difference is a multiple of 37.*

When solving a PHP problem:

1. Identify pigeons
2. Identify pigeonholes
3. Specify how pigeons are assigned to pigeonholes
4. Apply PHP

Pigeonhole Principle – Example (Surprising?)

In every set S of 100 integers, there are at least ***two*** *elements whose difference is a multiple of 37.*

When solving a PHP problem:

1. Identify pigeons
2. Identify pigeonholes
3. Specify how pigeons are assigned to pigeonholes
4. Apply PHP

Pigeons: integers x in S

Pigeonholes: $\{0,1,\ldots,36\}$

Assignment: x goes to $x \bmod 37$

Since $100 > 37$, by PHP, there are $x \neq y \in S$ s.t.
$x \bmod 37 = y \bmod 37$ which implies
$x - y = 37\,k$ for some integer k

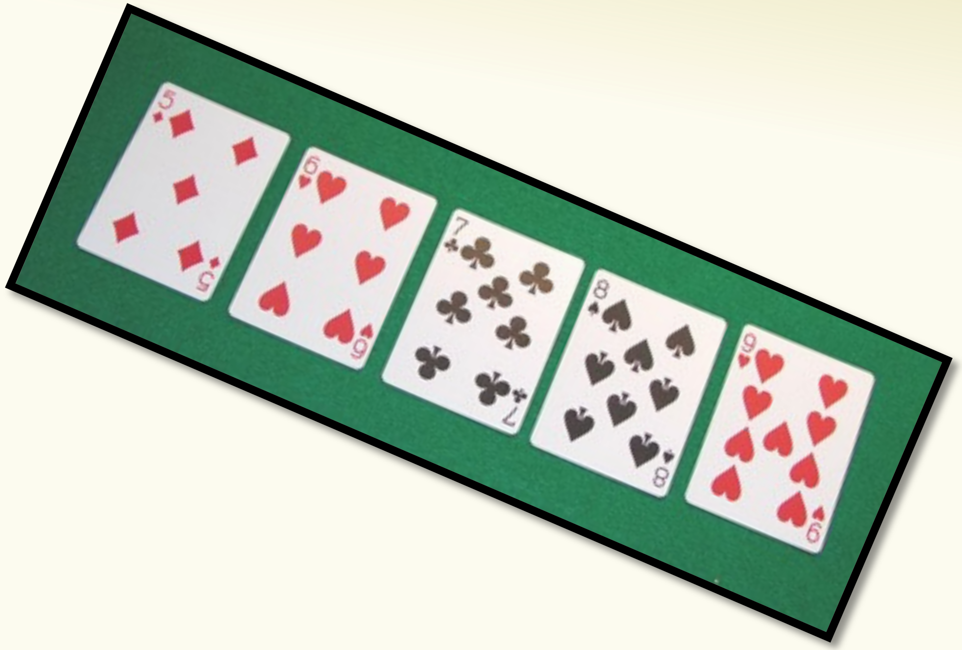
Last Class: Counting

- Binomial Coefficients
- Binomial Theorem
- Inclusion-Exclusion

Today:

- Pigeonhole Principle
- Counting practice

Quick Review of Cards



How many possible 5 card hands?

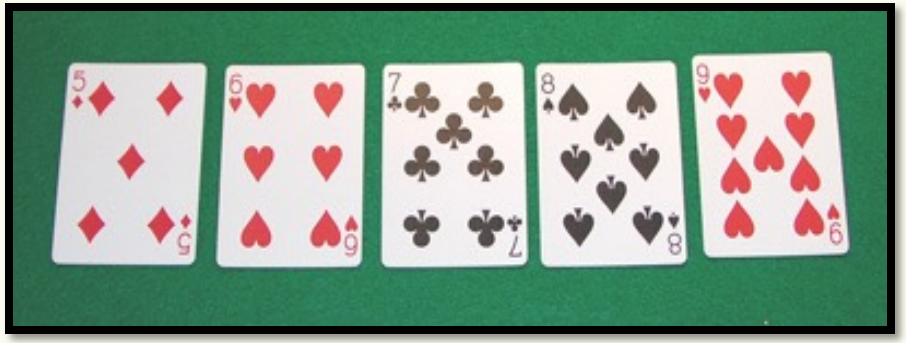
$$\binom{52}{5}$$

- 52 total cards
- 13 different ranks: 2,3,4,5,6,7,8,9,10,J,Q,K,A
- 4 different suits: Hearts, Diamonds, Clubs, Spades

Counting Cards I

- 52 total cards
- 13 different ranks: 2,3,4,5,6,7,8,9,10,J,Q,K,A
- 4 different suits: Hearts, Diamonds, Clubs, Spades

- A "straight" is five consecutive rank cards of any suit (where A,2,3,4,5 also counts as consecutive).
  How many possible straights?



$$10 \cdot 4^5 = 10{,}240$$

Counting Cards II

- 52 total cards
- 13 different ranks: 2,3,4,5,6,7,8,9,10,J,Q,K,A
- 4 different suits: Hearts, Diamonds, Clubs, Spades

- A flush is five card hand all of the same suit.

How many possible flushes?

$$4 \cdot \binom{13}{5} = 5148$$

Counting Cards III

- 52 total cards
- 13 different ranks: 2,3,4,5,6,7,8,9,10,J,Q,K,A
- 4 different suits: Hearts, Diamonds, Clubs, Spades

- A flush is five card hand all of the same suit.

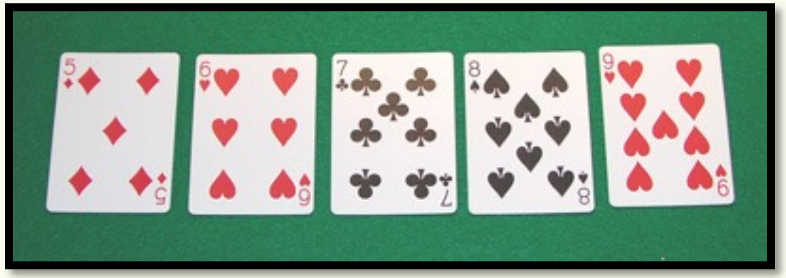
  How many possible flushes?

$$4 \cdot \binom{13}{5} = 5148$$

- How many flushes are NOT straights?

= #flush - #flush and straight

$$\left(4 \cdot \binom{13}{5} = 5148\right) - 10 \cdot 4$$



Sleuth's Criterion (Rudich)

For each object constructed, it should be possible to reconstruct the **unique** sequence of choices that led to it.

No sequence ➔ under counting   Many sequences ➔ over counting

EXAMPLE: How many ways are there to choose a 5 card hand that contains at least 3 Aces?

First choose 3 Aces. Then choose remaining two cards.

$$\binom{4}{3} \cdot \binom{49}{2}$$

Poll:

A. Correct
B. Overcount
C. Undercount

https://pollev.com/stefanotessaro617

Sleuth's Criterion (Rudich)

For each object constructed, it should be possible to reconstruct the **unique** sequence of choices that led to it.

Many sequences ➔ over counting

EXAMPLE: How many ways are there to choos

contains at least 3 Aces?

First choose 3 Aces. Then choose remaining two cards.

$$\binom{4}{3} \cdot \binom{49}{2}$$

Problem: This counts a hand with all 4 Aces in 4 different ways!

e.g. it counts ***A♣, A♦, A♥, A♠, 2♥***

four *times:*

{A♣, A♦, A♥} {A♠, 2♥}

{A♣, A♦, A♠} {A♥, 2♥}

{A♣, A♥, A♠} {A♦, 2♥}

{A♦, A♥, A♠} {A♣, 2♥}

Sleuth's Criterion (Rudich)

For each object constructed, it should be possible to reconstruct the **unique** sequence of choices that led to it.

No sequence ➔ under counting   Many sequences ➔ over counting

EXAMPLE: How many ways are there to choose a 5 card hand that contains at least 3 Aces?

Use the sum rule

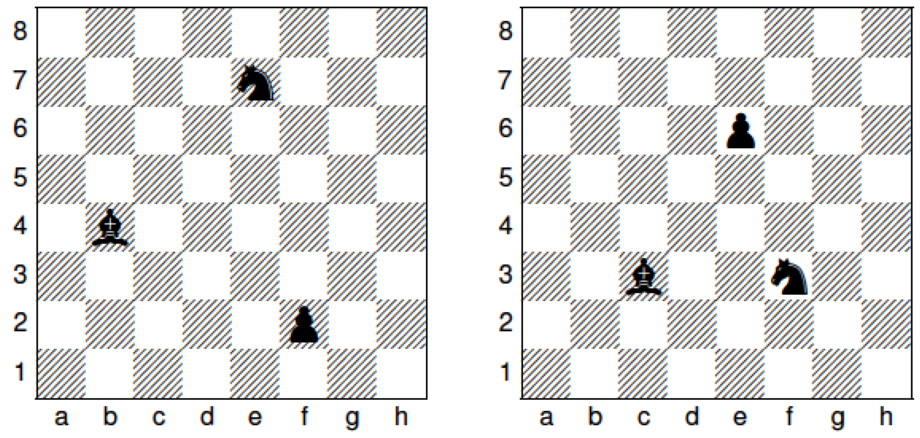
= # 5 card hand containing exactly 3 Aces $\binom{4}{3} \cdot \binom{48}{2}$

+ # 5 card hand containing exactly 4 Aces $\binom{48}{1}$

Random Picture

8 by 8 chessboard

How many ways to place a pawn, a bishop, and a knight so that none are in the same row or column ?



(a) valid (b) invalid

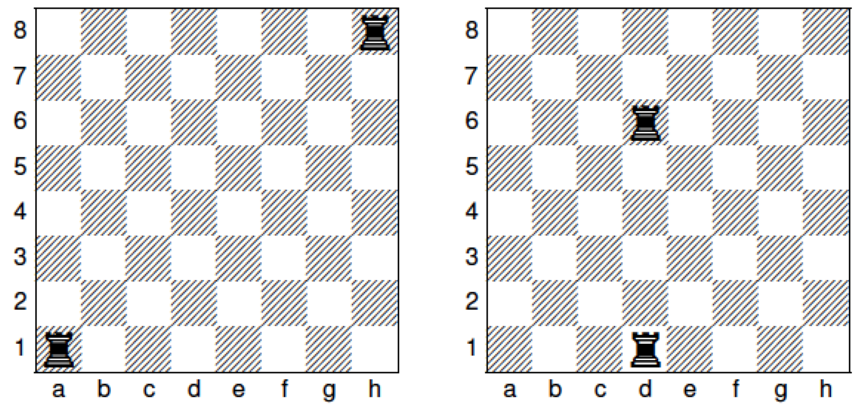
Sequential process:

1. Column for pawn
2. Row for pawn
3. Column for bishop
4. Row for bishop
5. Column for knight
6. Row for knight

$$(8 \cdot 7 \cdot 6)^2$$

Rooks on chessboard

How many ways to place two identical rooks on a chessboard so that they don't share a row or a column



(a) valid (b) invalid

Fully ordered: Pretend Rooks are different

1. Column for rook1
2. Row for rook1
3. Column for rook2
4. Row for rook2

$$(8 \cdot 7)^2$$

"Remove" the order of the two rooks:

$$(8 \cdot 7)^2/2$$

Counting when order only *partly* matters

We often want to count # of partly ordered lists:

Let M = # of ways to produce fully ordered lists

P = # of partly ordered lists

N = # of ways to produce corresponding fully ordered list given a partly ordered list

Then $M = P \cdot N$ by the product rule. Often M and N are easy to compute:

$$P = M/N$$

Dividing by N “removes” part of the order.

Anagrams (another look at rearranging SEATTLE)

How many ways can you arrange the letters in “Godoggy”?

$n = 7$ Letters, $k = 4$ Types {G, O, D, Y}

$n_1 = 3, n_2 = 2, n_3 = 1, n_4 = 1$

$$\frac{7!}{3!2!1!1!} = \binom{7}{3,2,1,1}$$

Multinomial coefficients

Multinomial Coefficients

If we have k types of objects ($\boldsymbol{n}$ total), with $\boldsymbol{n_1}$ of the first type, $\boldsymbol{n_2}$ of the second, …, and $\boldsymbol{n_k}$ of the k^{th}, then the number of orderings possible is

$$\binom{n}{n_1, n_2, \cdots, n_k} = \frac{n!}{n_1!\, n_2! \cdots n_k!}$$

*aka. "stars and bars method"

Counting using binary encoding*

The number of ways to distribute n indistinguishable balls into k distinguishable bins is

$$\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$$

E.g., = # of ways to add k non-negative integers up to n

Coins

How many ways can you distribute 32 identical coins among Alex, Barbara, Charlie, Dana, and Eve?

1. Identify balls
2. Identify bins

$$\binom{32+5-1}{5-1}$$

Binomial Theorem

Theorem. Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$ a positive integer. Then,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Corollary.

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Binomial Theorem: A less obvious consequence

Theorem. Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$ a positive integer. Then,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

= -1 if k is odd
= $+1$ if k is even

Corollary. For every n, if O and E are the sets of odd and even integers between 0 and n

$$\sum_{k \in O} \binom{n}{k} = \sum_{k \in E} \binom{n}{k}$$

e.g., n=4: 1 4 6 4 1

Proof: Set $x = -1, y = 1$ in the binomial theorem

Tools and concepts

- Sum rule, Product rule
- Permutations, combinations
- Inclusion-exclusion
- Binomial Theorem
- Combinatorial proofs
- Pigeonhole principle
- Binary encoding/stars and bars